JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS and Junos OS Evolved: When an unsigned Python op script configuration is present, a local low privileged user can compromise the system (CVE-2026-33793)

Article ID JSA103142 **Created** 2026-04-08 **Last Updated** 2026-04-16

Product Affected

This issue affects all versions of Junos OS. This issue affects all versions of Junos OS Evolved.

Severity
High

Severity Assessment (CVSS) Score
CVSS: v3.1: 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) **CVSS: v4.0:** 8.5 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/R:U/V:C/RE:M/U:Amber)

Problem

An Execution with Unnecessary Privileges vulnerability in the User Interface (UI) of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to gain root privileges, thus compromising the system.

When a configuration that allows unsigned Python op scripts is present on the device, a non-root user is able to execute malicious op scripts as a root-equivalent user, leading to privilege escalation.

This issue affects Junos OS:

- All versions before 22.4R3-S7,
- from 23.2 before 23.2R2-S4,
- from 23.4 before 23.4R2-S6,
- from 24.2 before 24.2R1-S2, 24.2R2,
- from 24.4 before 24.4R1-S2, 24.4R2;

Junos OS Evolved:

- All versions before 22.4R3-S7-EVO,
- from 23.2 before 23.2R2-S4-EVO,
- from 23.4 before 23.4R2-S6-EVO,
- from 24.2 before 24.2R2-EVO,
- from 24.4 before 24.4R1-S1-EVO, 24.4R2-EVO.

This issue can affect all systems with Python 3 op scripts enabled:

```
[ system scripts language python3 ]
```

However, the risk of malicious exploitation is significantly higher when the ability to execute Python 3 op scripts from a remote location is enabled:

```
[ system scripts op allow-url-for-python ]
```

Starting in Junos OS Evolved Release 21.2R1, the `junos-defaults` configuration group includes '`system scripts language python3`' enabled by default.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.
This issue was found during internal product security testing or research.

Solution

The following software releases have been updated to resolve this specific issue:

Junos OS Evolved: 22.4R3-S7-EVO, 23.2R2-S4-EVO, 23.4R2-S6-EVO, 24.2R2-EVO, 24.4R1-S1-EVO, 24.4R2-EVO, 25.2R1-EVO and all subsequent releases.

Junos OS: 22.4R3-S7, 23.2R2-S4, 23.4R2-S6, 24.2R1-S2, 24.2R2, 24.4R1-S2, 24.4R2, 25.2R1 and all subsequent releases.

This issue is being tracked as 1842247 which is visible on the Customer Support website.
Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

Workaround

Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators.

Severity Assessment

Information for how Juniper Networks uses CVSS can be found at KB 16446, "Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories."

Modification History

```
2026-04-08: Initial Publication
2026-04-16: While 'language python3' allows an attacker to execute local Python
scripts, the scenario with the highest risk of malicious exploitation occurs when
an attacker can execute remote Python scripts
```

Related Information

- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?

- KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories
- Report a Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- https://www.cve.org/CVERecord?id=CVE-2026-33793

AFFECTED PRODUCT SERIES / FEATURES